WHAT IS CLAIMED IS:

1. A storage device comprising:

a storage medium for retaining data; and

a cryptographic processing unit which receives a plurality of commands from a host device to execute the commands upon performing a plurality of series of cryptographic input/output processing for encrypting data to be secured and inputting/outputting the data between the storage medium and a host device, the commands being issued by dividing the plurality of series of cryptographic input/output processing each into a plurality of procedures, wherein

the cryptographic processing unit refers to identifying information attached to the command to identify to which cryptographic input/output processing the command belongs to, then simultaneously performing two or more of the plurality of cryptographic input/output processing procedures.

2. The storage device according to claim 1, wherein

the cryptographic processing unit manages the sequence of commands executed in each cryptographic input/output processing and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command.

3. The storage device according to claim 2, wherein

when the cryptographic processing unit receives the incorrectly sequenced command, the cryptographic processing unit interrupts the cryptographic input/output processing to which the command belongs.

4. The storage device according to claim 1, wherein

the number of the cryptographic input/output processing which can be performed simultaneously by the storage device is predetermined in accordance with a performance of the storage device.

5. The storage device according to claim 1, wherein

in response to a request from the host device, the storage device provides to the host device the maximum number of cryptographic input/output processing which can be performed simultaneously by the storage device.

6. The storage device according to claim 1, wherein

the storage medium comprises a normal data storing unit and a confidential data storing unit, the normal data storing unit storing normal data to be exchanged bypassing the cryptographic processing unit, the confidential data storing unit storing the secret data to be exchanged via the cryptographic processing unit.

7. A storage device comprising:

a storage medium for retaining data; and

a cryptographic processing unit for receiving a plurality of commands from a host device to execute the commands upon performing a series of cryptographic input/output processing for encrypting data to be secured and inputting/outputting the data between the storage medium and the host device, the commands being issued by dividing the series of cryptographic input/output processing into a plurality of procedures, wherein

the cryptographic processing unit can manage two or more cryptographic input/output processings, and refer to identifying information attached to the command to identify to which cryptographic input/output processing the received command belongs to, and rejects the execution of the command when having detected that the command is an incorrectly sequenced command in the cryptographic input/output processing to which the command belongs.

8. The storage device according to claim 7, wherein

in response to a request from the host device, the storage device provides to the host device the maximum number of cryptographic input/output processings which can be performed simultaneously by the storage device.

9. The storage device according to claim 7, wherein

the storage medium comprises a normal data storing unit and a confidential data storing unit, the normal data storing unit storing normal data to be exchanged bypassing the cryptographic processing unit, the confidential data storing unit storing the secret data to be exchanged via the cryptographic processing unit.

10. A host device which exchanges data with a storage device that is capable of simultaneously performing a plurality of series of cryptographic input/output processing for encrypting data to be secured and inputting/outputting the data, the host device comprising:

a controller which divides the cryptographic input/output processing into a plurality of procedures and issuing commands sequentially to the storage device thereby allowing the storage device in order to make the storage device execute a procedure to be executed on the storage-device side; and

a cryptographic processing unit which carries out encryption or decryption that is required of the cryptographic input/output processing, wherein

when the controller issues a command, the controller attaches identifying information to the command to identify to which one of the plurality of cryptographic input/output processings the command belongs.

11. The host device according to claim 10, wherein

the controller issues a command to allocate a process system for performing the cryptographic input/output processing prior to initiation of the cryptographic input/output processing.

12. A data input/output method, when performing cryptographic input/output processing between a host device and a storage device that is capable of simultaneously performing a plurality of series of cryptographic input/output processing for encrypting data to be secured and inputting/outputting the data, and storing data to be exchanged through the cryptographic input/output processing, comprising:

dividing the cryptographic input/output processing divided into a plurality of procedures and allowing the host device to execute a procedure to be executed on the host-device side out of the procedures;

allowing the host device to issue a command to the storage device in order to make the storage device execute a procedure to be executed on the storage-device side;

allowing the storage device to receive the command; and

allowing the storage device to execute the command, wherein

identifying information is attached to the command to identify to which one of the plurality of cryptographic input/output processings, being performed simultaneously by the storage device, the command belongs.

13. The data input/output method according to claim 12, further comprising predetermining an upper-limit number of the cryptographic input/output processings that can be performed simultaneously by the storage device in accordance with performance of the storage device.

14. The data input/output method according to claim 12, further comprising:

allowing the storage device to predetermine an upper-limit number of the cryptographic input/output processings that the storage device can perform simultaneously in accordance with its own performance, and

informing the host device of the upper limit.

15. The data input/output method according to claim 13, further comprising, prior to performing the cryptographic input/output processing, selecting and allocating identifying information for identifying the cryptographic input/output processing to be performed from among the prepared number of pieces of identifying information determined in the determining step.

16. The data input/output method according to claim 14, further comprising, prior to performing the cryptographic input/output processing, selecting and allocating identifying information for identifying the cryptographic input/output processing to be performed from among the prepared number of pieces of identifying information determined in the determining step.

17. The data input/output method according to claim 12, wherein

the receiving step comprises:

determining whether the received command is a correctly sequenced command in the cryptographic input/output processing;

accepting the command successfully when the received command has been determined to be a correctly sequenced command; and

rejecting the execution of the received command when the received command has been determined to be an incorrectly sequenced command.

18. The data input/output method according to claim 17, wherein

when the received command has been determined to be an incorrectly sequenced command, the execution of the

cryptographic input/output processing to which the command belongs is interrupted.